Morphing Attack Detection Overview

Christoph Busch, Ulrich Scherhag, Christian Rathgeb,
Kiran Raja, Raghu Ramachandra, Marta Gomez-Barrero,
Daniel Fischer, Sergey Isadskiy

copy of slides available at:
https://www.christoph-busch.de/projects-mad.html

NIST-IFPC-2018, November 28, 2018

CRISP
Center for Research
in Security and Privacy

European
Association for
Biometrics
eab
Human Identity in Europe

NTNU

Overview

Agenda

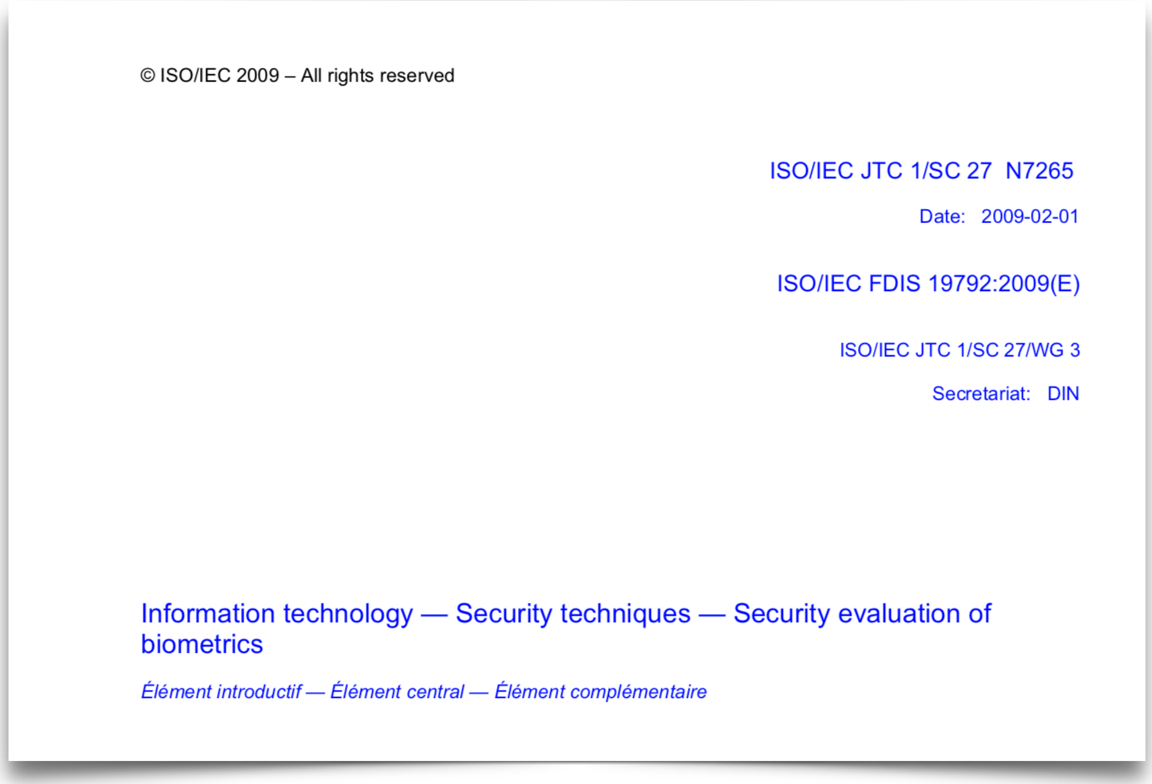
- Introduction - Problem description
- Morphing Attack Detection - Scenarios and Methods
- Status: Face Morphing Attack Detection
- Future - what needs to be done?
- Conclusion

Problem Description

History - 2009

Face Morphing

- The morphing attack was named and classified as vulnerability of a biometric system in Clause 8.3.8.1 of ISO/IEC FDIS 19792:
  - *"… Examples of abnormal characteristics could include those with unusually large or small numbers of features. Such characteristics may not be representative of any human biometric characteristic but could be synthesised and copied to an artefact. Alternatively a synthesised characteristic could be injected electrically during a replay attack or planted in the reference database.*
    ….
    - feature sets comprising amalgamations of biometric features from 2 or more individuals, e.g. morphed facial images"



ISO/IEC JTC 1/SC 27 N7265

Date: 2009-02-01

ISO/IEC FDIS 19792:2009(E)

ISO/IEC JTC 1/SC 27/WG 3

Secretariat: DIN

Information technology — Security techniques — Security evaluation of biometrics

Élément introductif — Élément central — Élément complémentaire

History - 2014

Integrated Project FIDELITY

http://www.fidelity-project.eu/

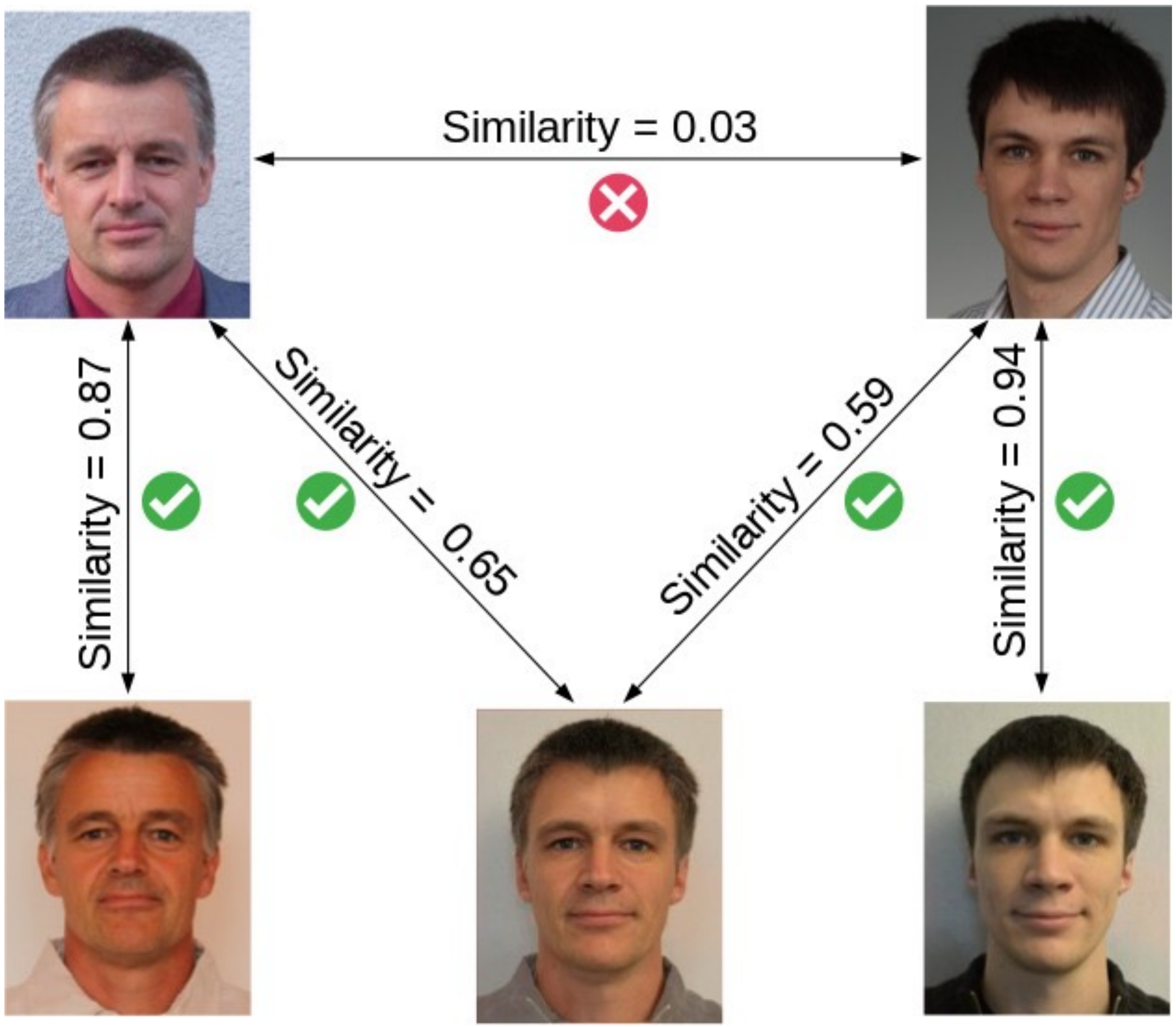
- Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy
- 4 years project (2012-2016)
  - European 7th Framework Programme
- Objectives:
  - To improve the ePassport issuing process
    - Security of birth certificates and other evidence of identity
    - Quality of biometric data in the chip
    - One individual one passport (duplicate enrolment check)
  - To demonstrate solutions that enable faster and more secure and efficient real-time authentication of individuals at border crossing
  - To protect privacy of the travel document holders with a privacy-by-design approach.

Problem: Morphing Attacks

Verification against morphed facial images

Probe sample of A

Probe sample of C



Enrolment sample of A

Enrolment sample of C

Enrolment morph M

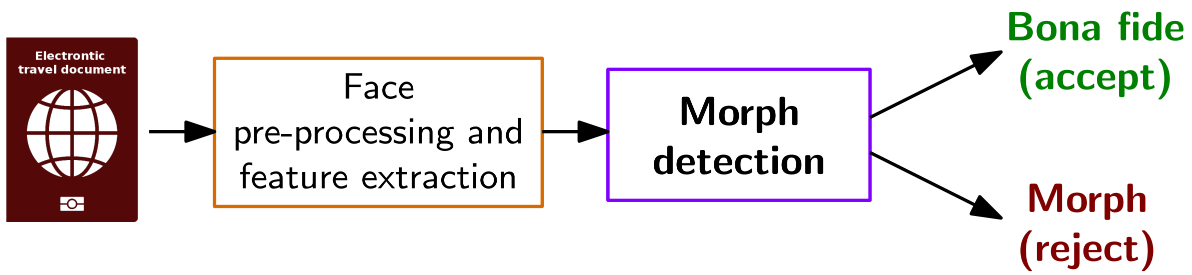
Morphing Attack Detection (MAD)

Scenarios and Methods

Morphing Attack Detection Scenarios

Real world scenarios

- No-reference morph detection
  - One single facial image is analysed (e.g. in the passport application office)

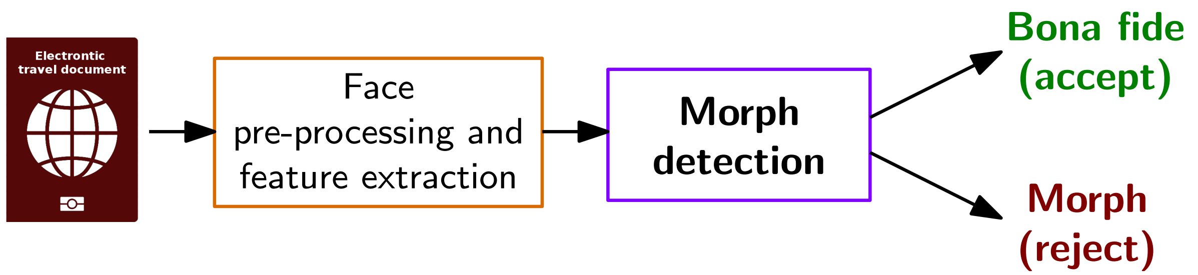


[SRB18a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

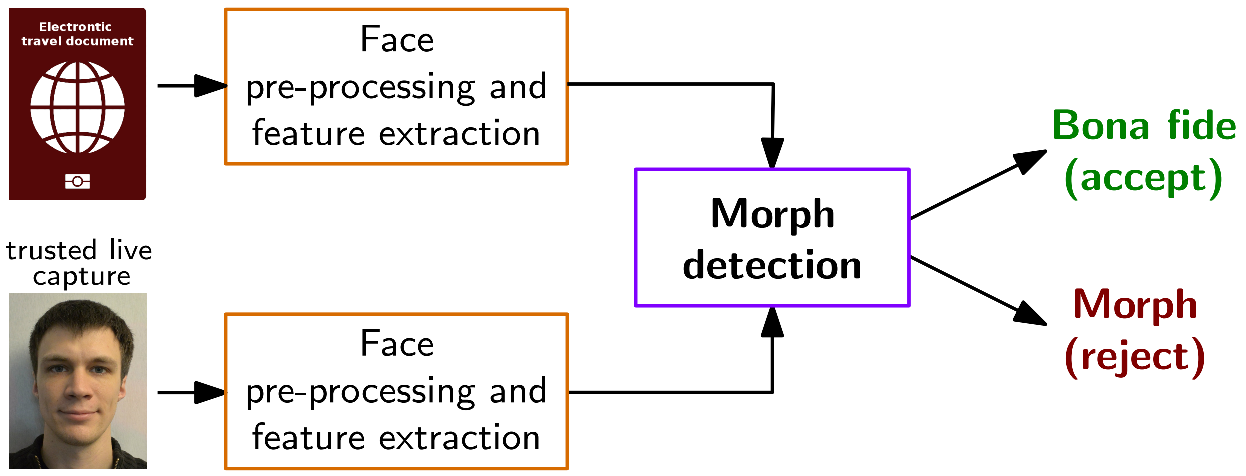
Morphing Attack Detection Scenarios

Real world scenarios

- No-reference morph detection
  - One single facial image is analysed (e.g. in the passport application office)



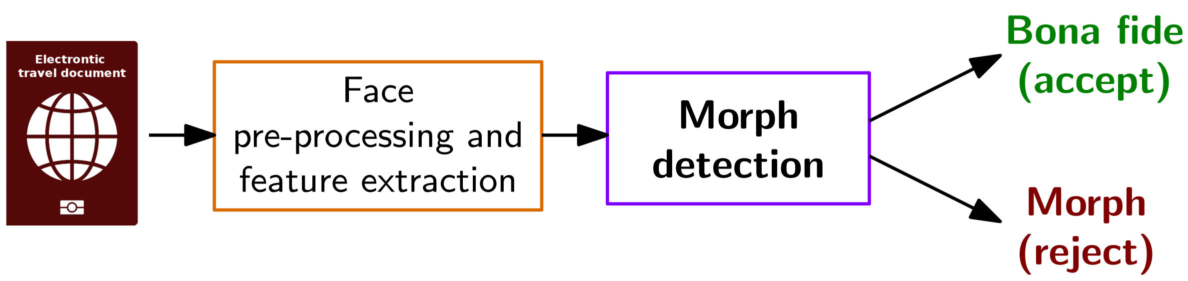
- Differential morph detection
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)



[SRB18a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as hand-crafted features

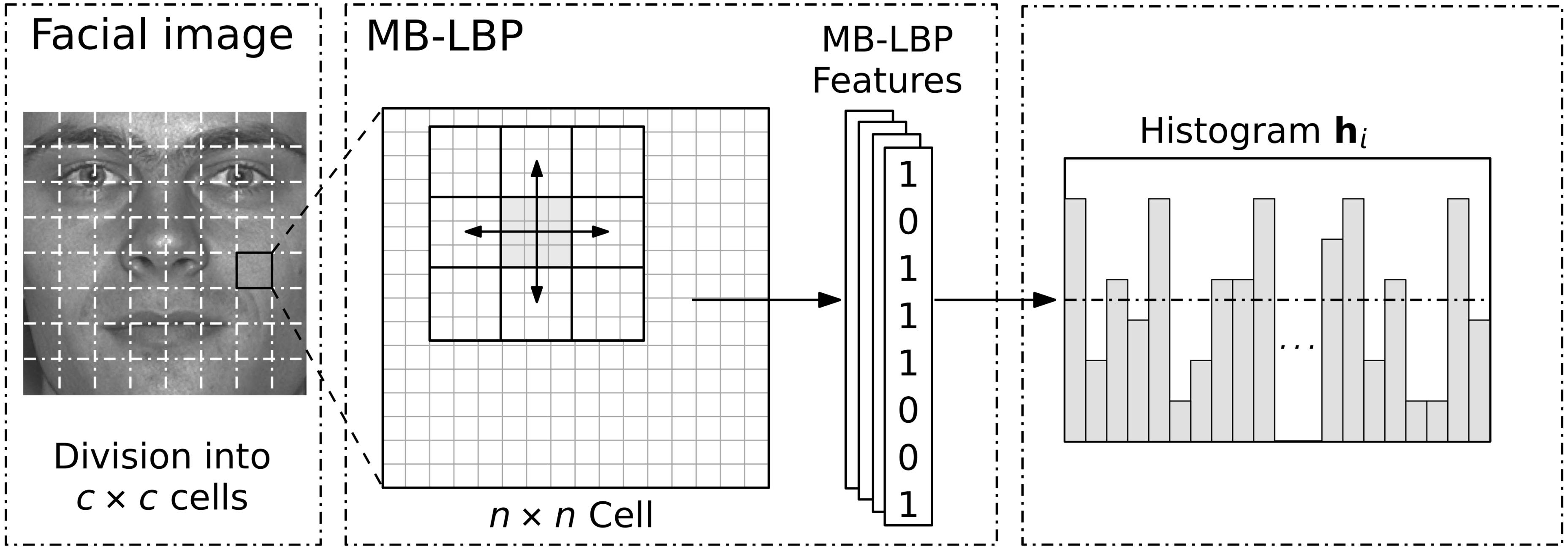


[SRB18b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)

Face Pre-processing and Feature Extraction

MAD with image descriptor

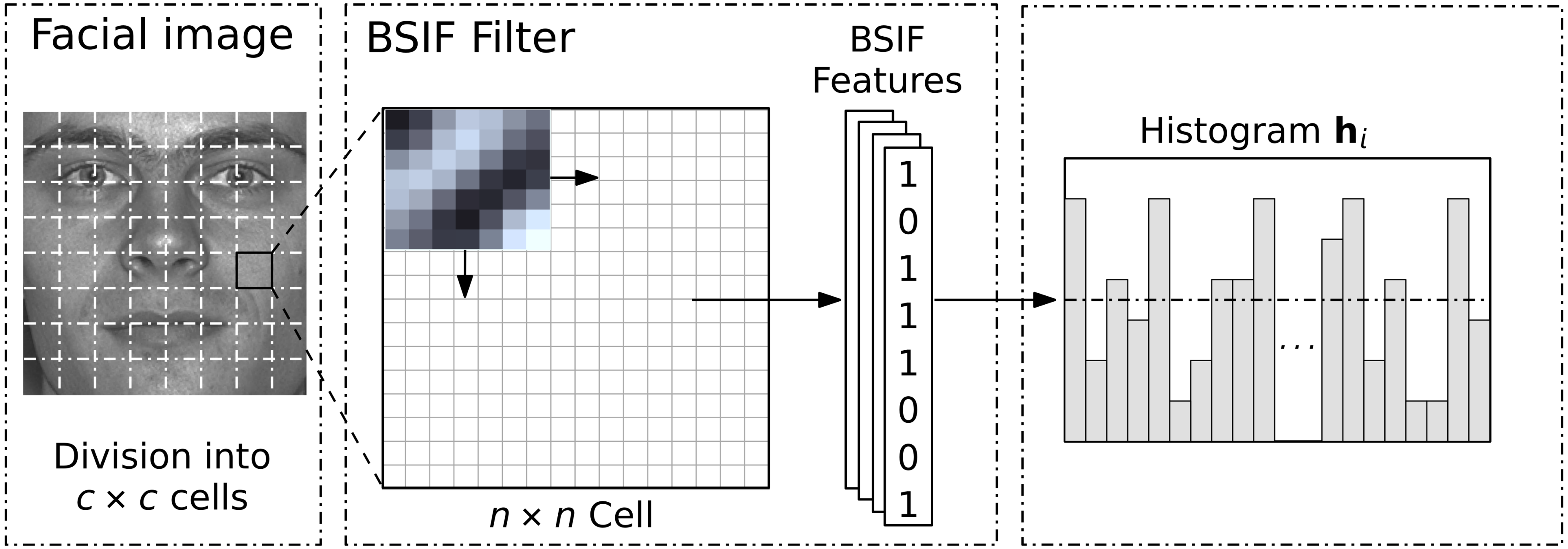
- Local Binary Pattern (LBP)



Face Pre-processing and Feature Extraction

MAD with image descriptor

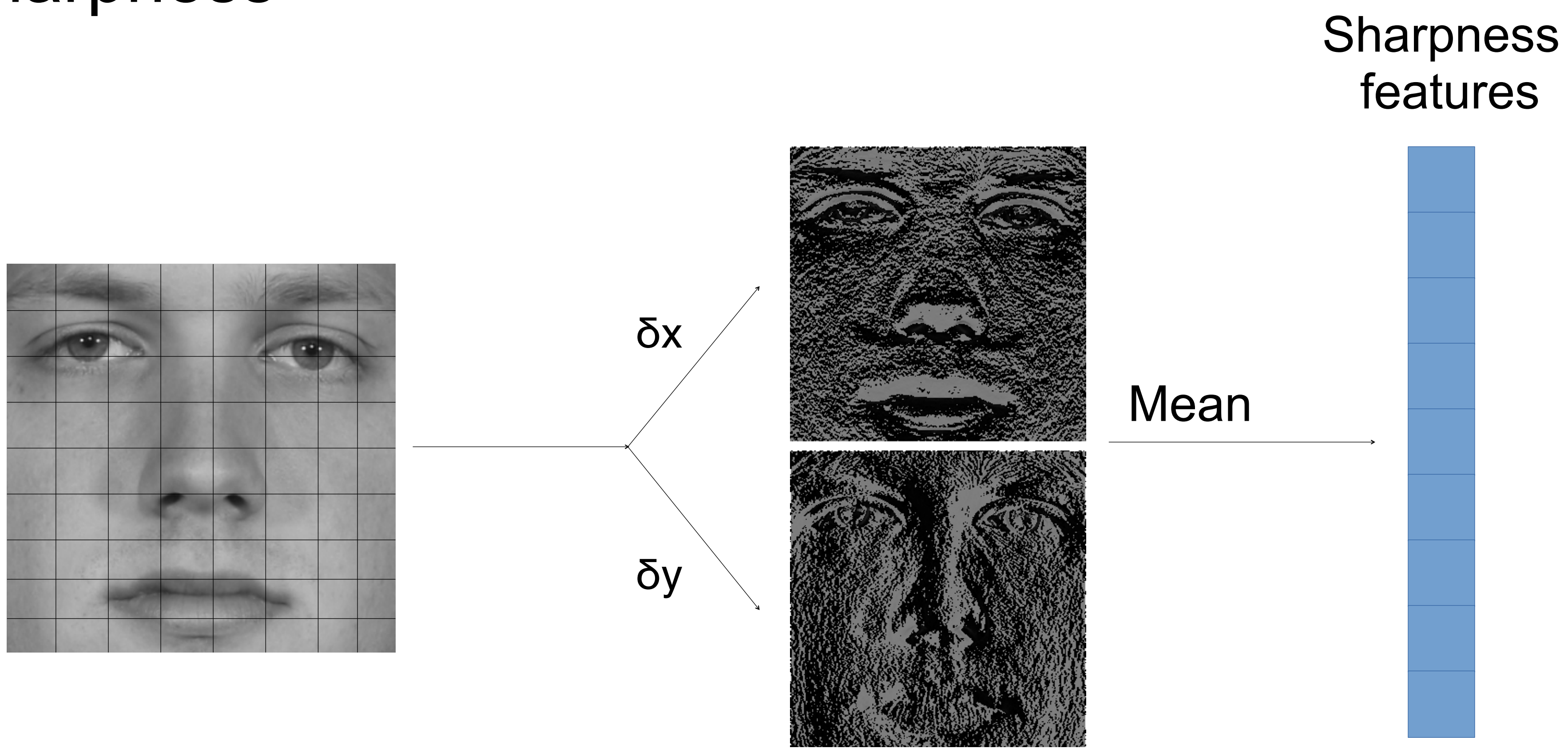
- Binarized Statistical Image Features (BSIF)



Face Pre-processing and Feature Extraction

MAD with image descriptor

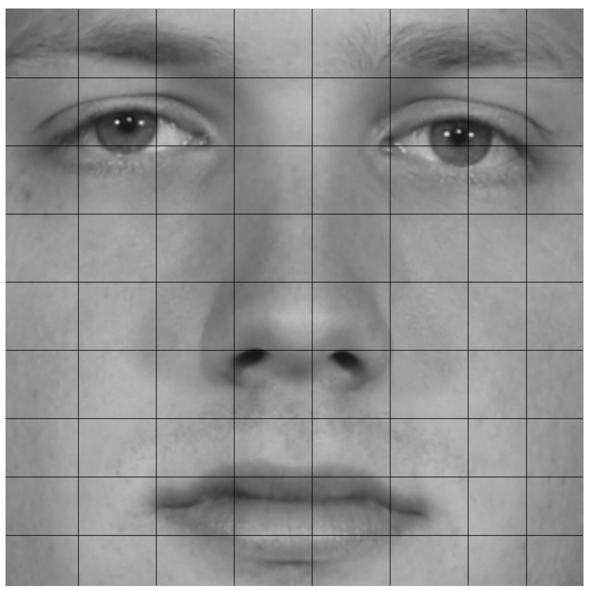
- Sharpness

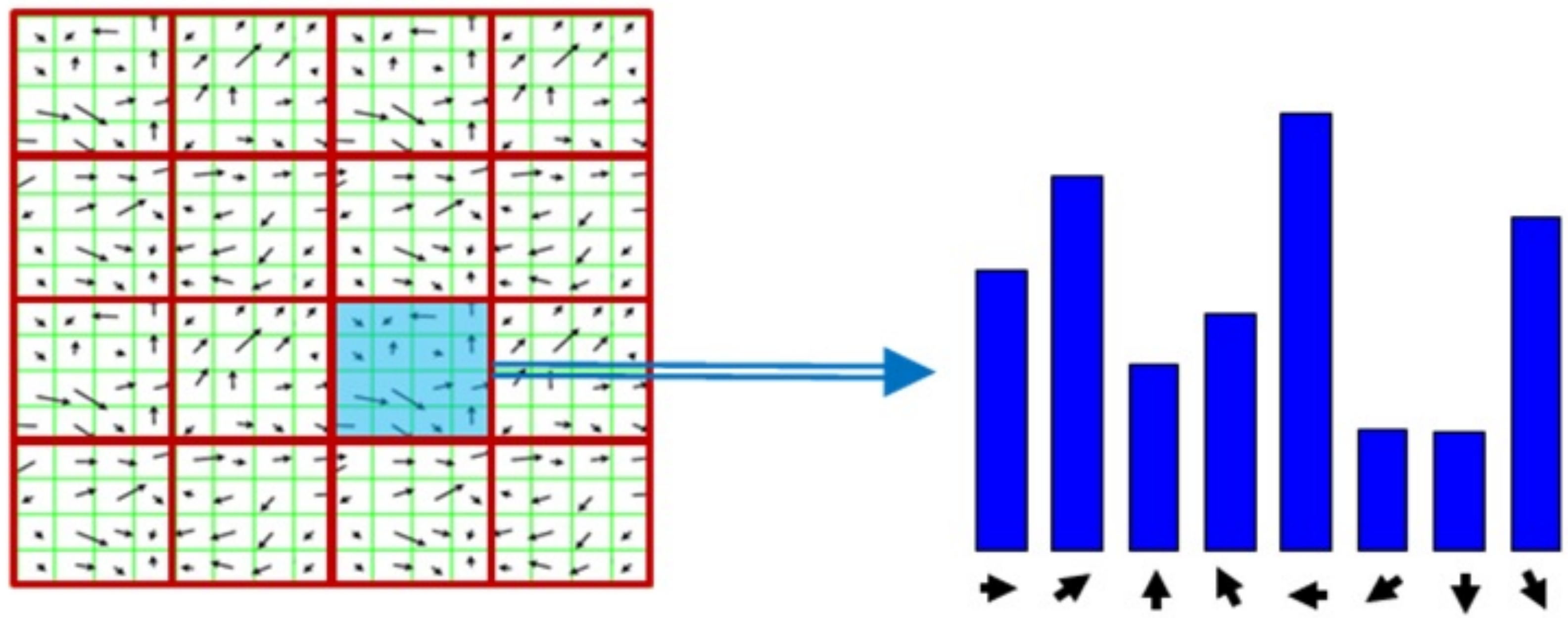


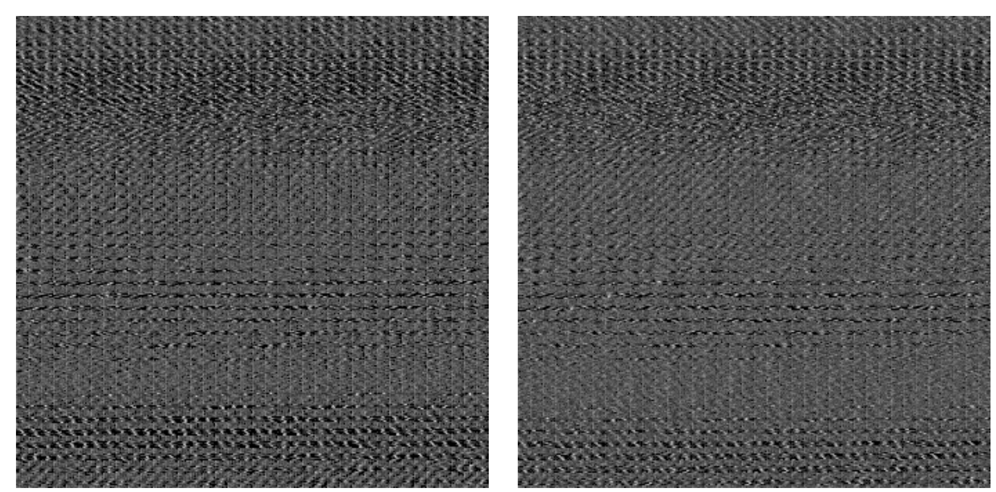
Face Pre-processing and Feature Extraction

MAD with image descriptor

- Histogram of Gradients (HOG)





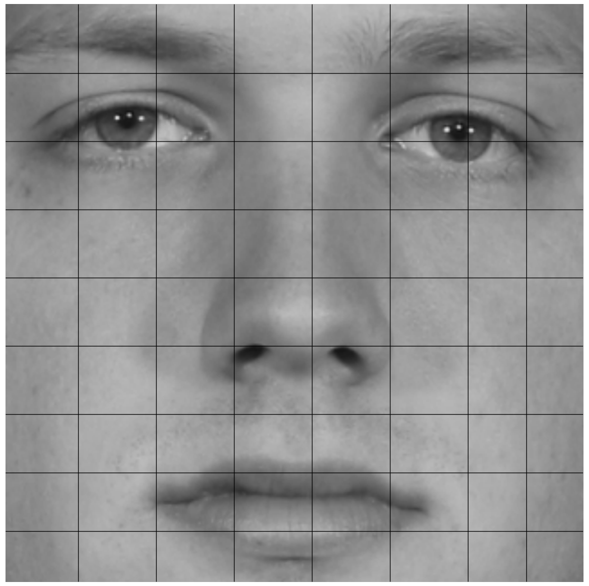


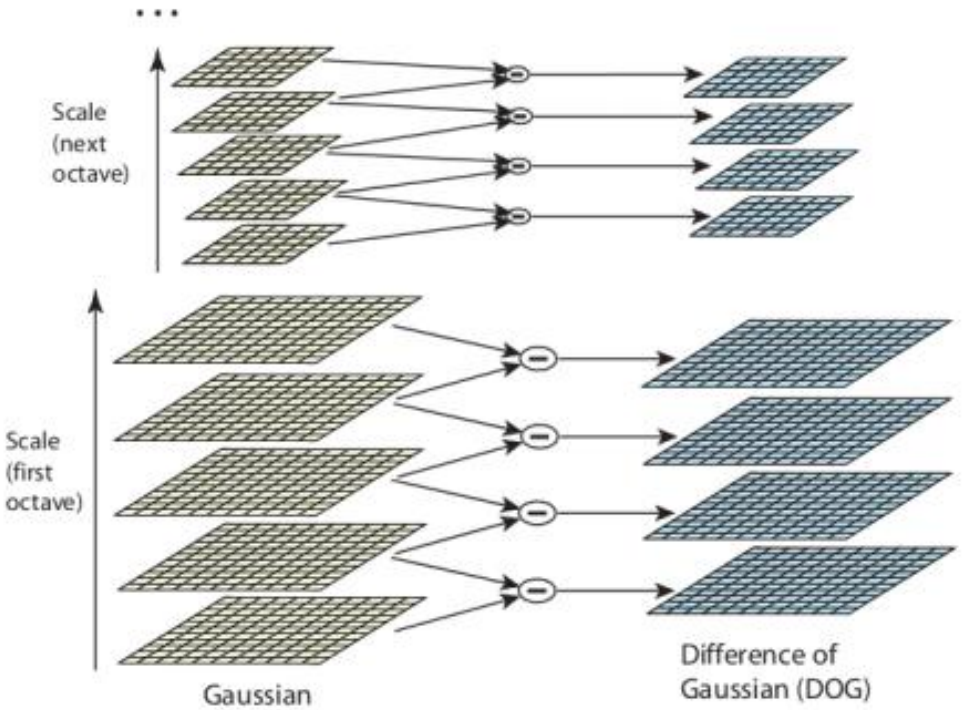
Morph Bona Fide

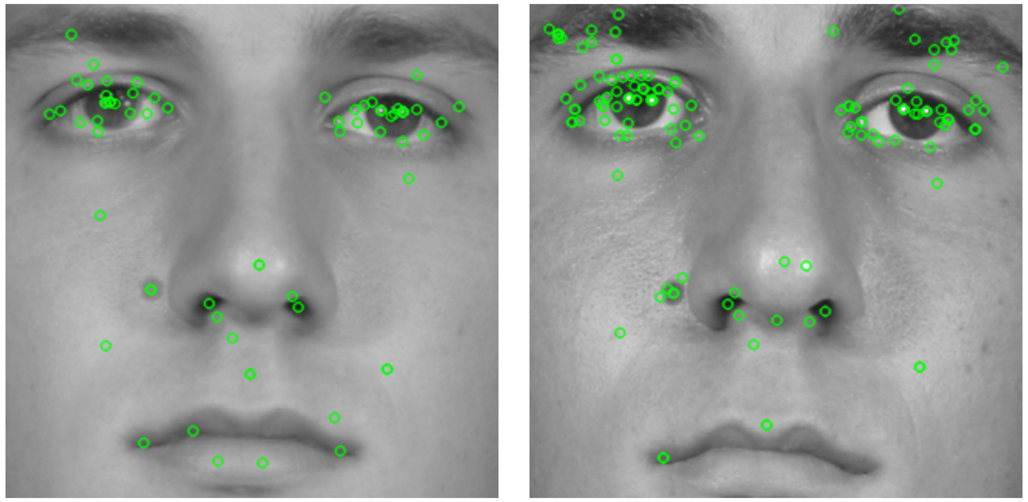
Face Pre-processing and Feature Extraction

MAD with image descriptor

- Scale Invariant Feature Transform (SIFT)
- Speeded up Robust Features (SURF)





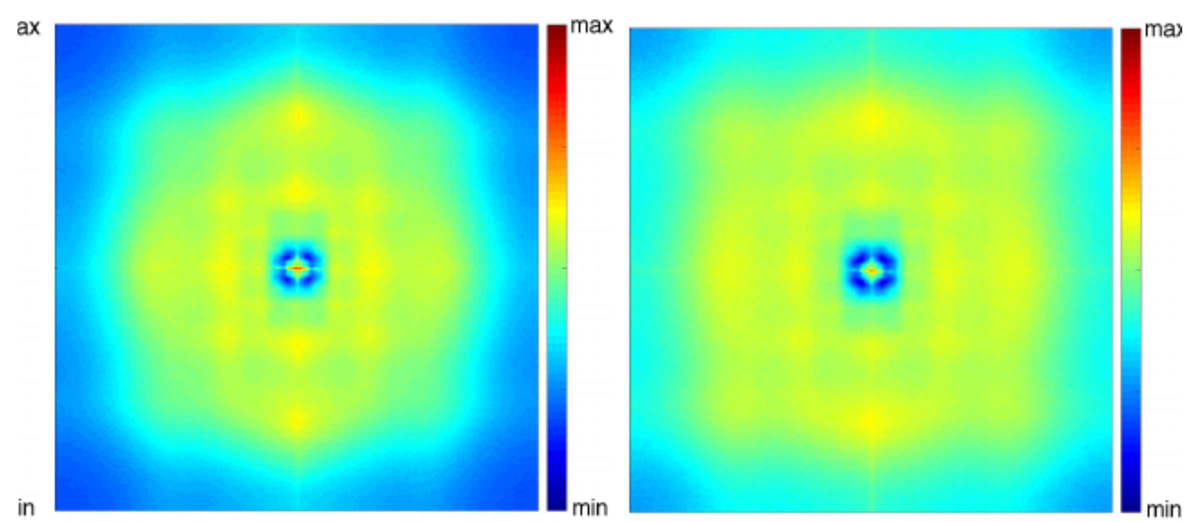


Morph Bona Fide

Face Pre-processing and Feature Extraction

MAD with image descriptor / forensic approach

- Photo Response Non-Uniformity (PRNU)

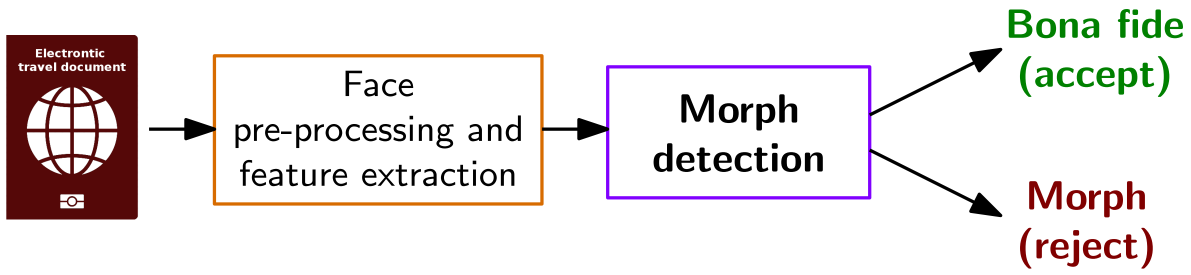


Morph Bona Fide

Face Pre-processing and Feature Extraction

Morphing Attack Detection (MAD) with texture analysis

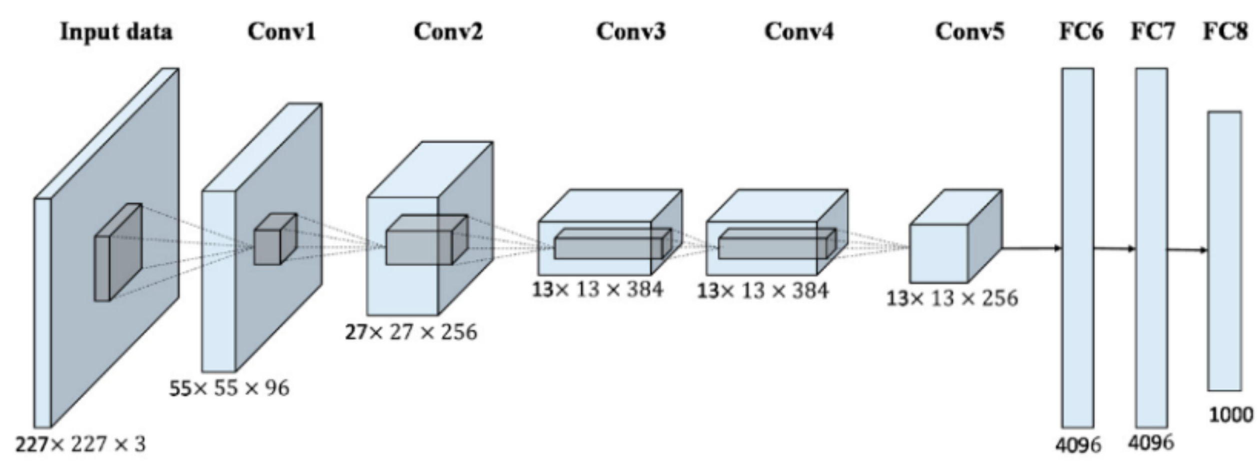
- Image descriptors as Deep features



Face Pre-processing and Feature Extraction

MAD with deep learning

- Deep Features
  - pre-trained Convolutional Neural Network (CNN)
  - OpenFace



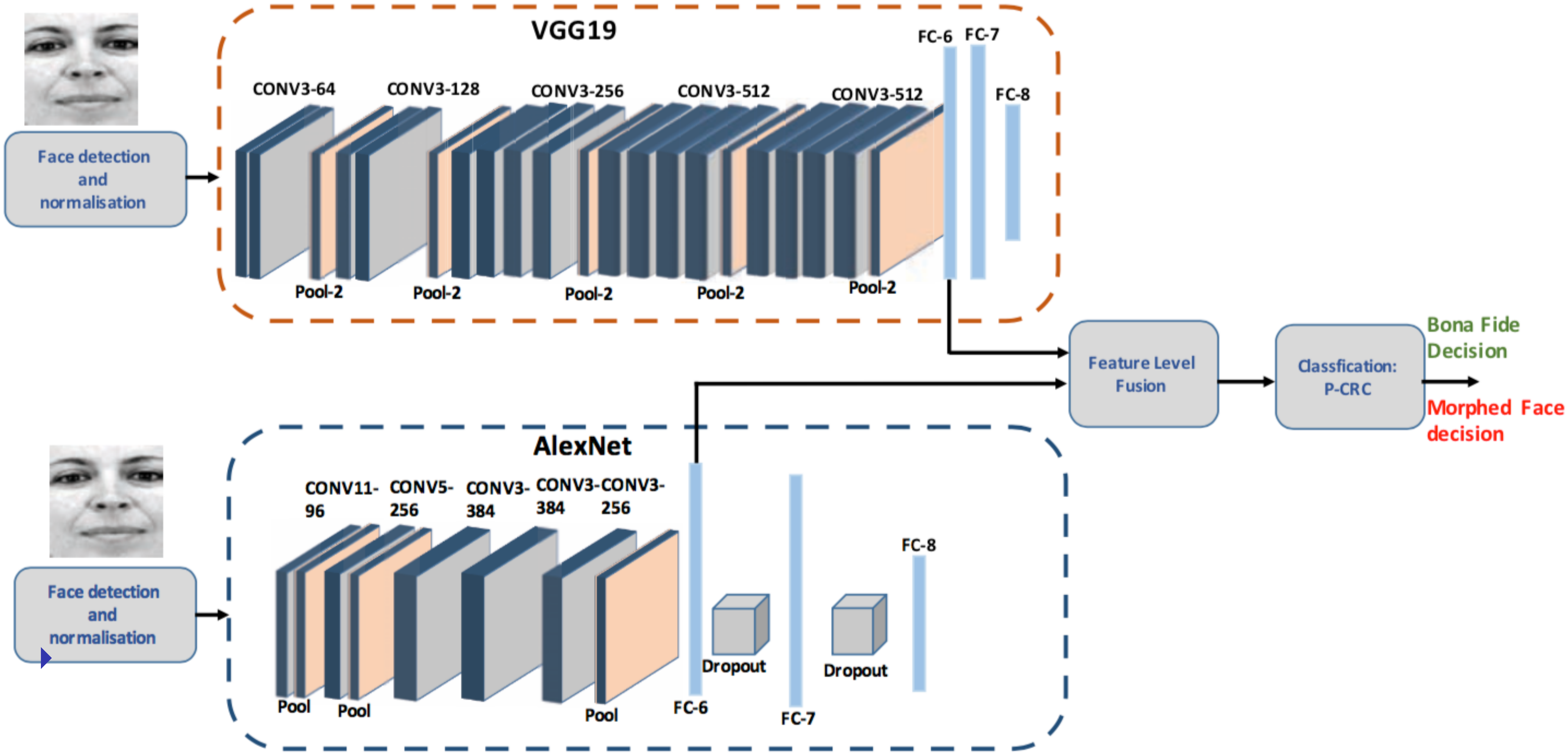
Morph Detection Classifier

[Amos16] B. Amos, B. Ludwiczuk und M. Satyanarayanan: „Open-Face: A general-purpose face recognition library with mobile applications“, Technical report, CMU School of Computer Science, (2016)

No-Reference Morph Detection

MAD with deep learning

- Feature level fusion of Deep CNNs



[RRVBu17] R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), July 21-26, (2017)

MAD Evaluation Methodology

MAD Evaluation Methodology

Face Morphing Attack evaluations are complex

- Evaluations must consider a dedicated methodology
  - see the following presentation by Marta Gomez-Barrero [SNR17]

[SNR17] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 20-22, (2017)

MAD Evaluation Methodology

Evaluations must consider many parameters

result = f (dataset-training, dataset-testing, morphing-attack, landmark-detector, feature-extractor, classifier, scenario (no-reference vs. differential), post-processing, printer, scanner)

Quality of the passport image under investigation
- hopefully ICAO 9303 compliant
and
- ISO/IEC 39794-5 compliant

MAD Evaluation Methodology

Evaluations must consider many parameters

- For a differential MAD evaluation

result = f (dataset-training, dataset-testing, morphing-attack, landmark-detector, feature-extractor, classifier, scenario (no-reference vs. differential), post-processing, printer, scanner)

Quality of the passport image under investigation and quality of the trusted probe image

In our evaluation we use

- The FERET dataset for training
  https://www.nist.gov/programs-projects/face-recognition-technology-feret
- The FRGCv2 dataset for testing
  https://www.nist.gov/programs-projects/face-recognition-grand-challenge-frgc
- Both data sets were filtered to reach ICAO compliance

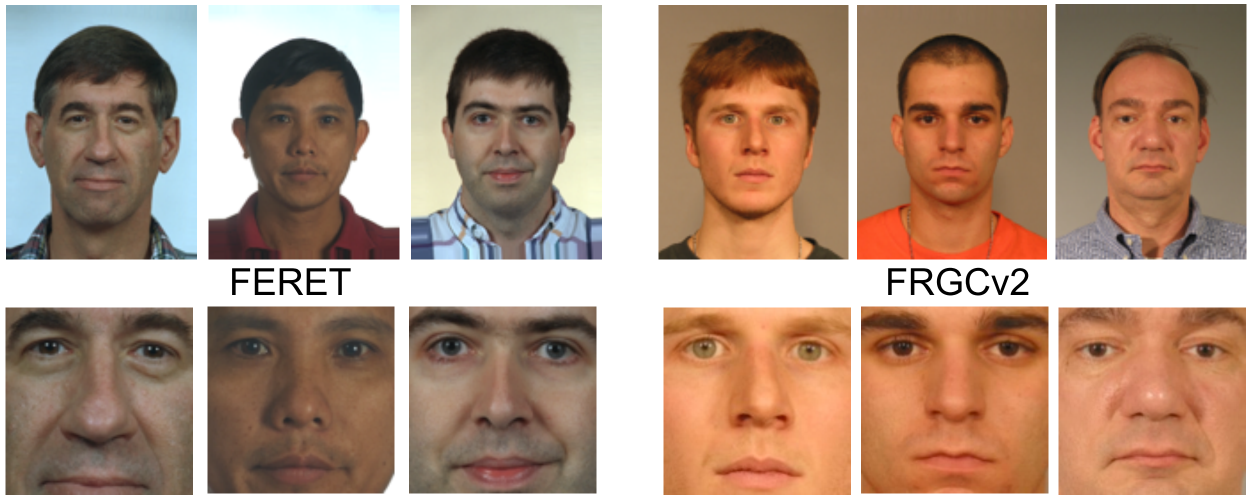
MAD Evaluation Methodology

Evaluations must consider many parameters

- Dataset preparation requires pre-processing

result = f (dataset-training, dataset-testing, morphing-attack, landmark-detector, feature-extractor, classifier, scenario (no-reference vs. differential), post-processing, printer, scanner)

Facial images are cropped and aligned
to a normalized size



Resulting images are

- cropped tp 320x320 pixel
- aligned according to Dlib landmarks, such that eyes are at identical coordinates

MAD Evaluation Methodology

Evaluations must consider many parameters

- Morphing may require manual interaction (not desired)

result = f (dataset-training, dataset-testing, morphing-attack, landmark-detector, feature-extractor, classifier, scenario (no-reference vs. differential), post-processing, printer, scanner)

Automated face morphing tools may introduce artifacts

In our evaluation we use

- Dlib / OpenCV
- FaceMorpher

Subject 1 | Morph (Dlib and OpenCV) | Morph (FaceMorpher) | Subject 2

MAD Evaluation Methodology

Evaluations must consider many parameters

- From machine learning tools we select a classifier

result = f (dataset-training, dataset-testing, morphing-attack,
landmark-detector, feature-extractor, classifier,
scenario (no-reference vs. differential),
post-processing, printer, scanner)

Simplicity and generalisation capability are desired properties

In our evaluation we use

- Support Vector Machine (SVM)
  - with radial basis function as kernel
- AdaBoost
  - with 200 estimates and a decision stump

MAD Evaluation Methodology

Evaluations must consider many parameters

- Postprocessing might conceal morphing effects (e.g. smoothing)

result = f (dataset-training, dataset-testing, morphing-attack, landmark-detector, feature-extractor, classifier, scenario (no-reference vs. differential), post-processing, printer, scanner)

smoothing and other effects might be compensated by the attacker

Morph Sharpening Histogram equalisation

In our evaluation we show results for

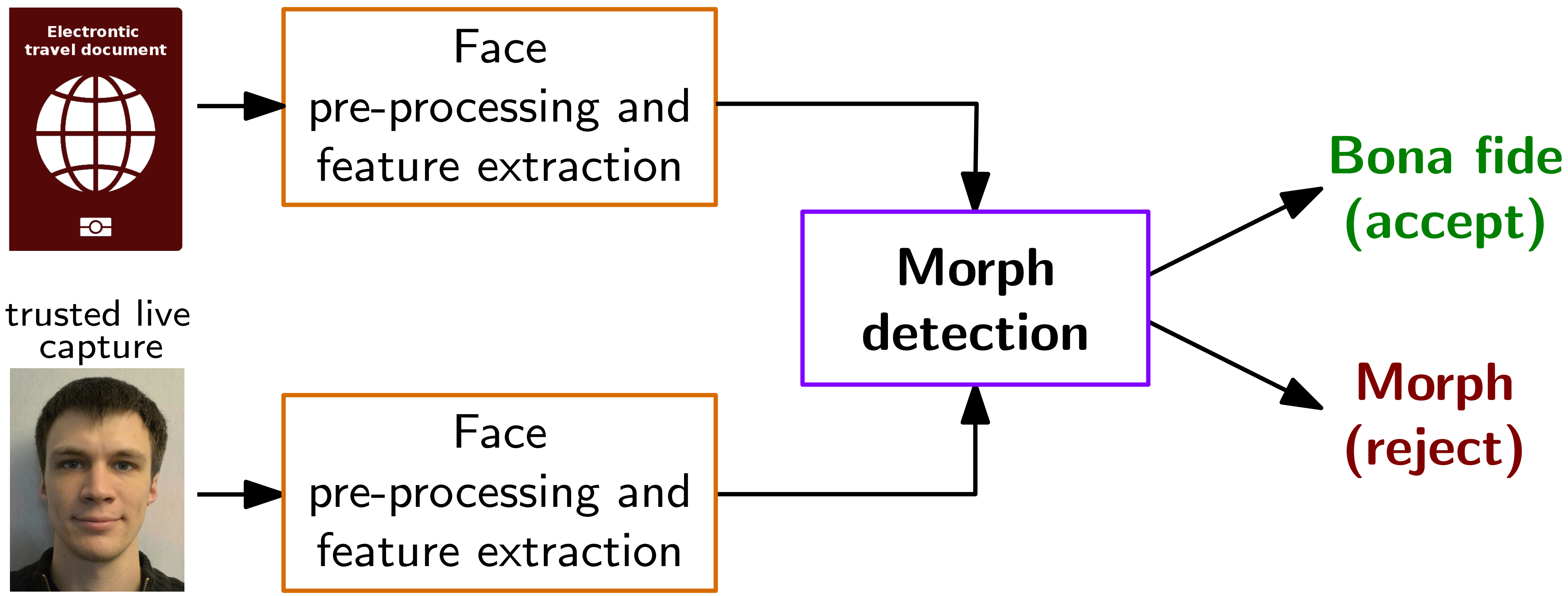
- Sharpening

Results

MAD Evaluation

Generalising evaluation - differential scenario

- Differential morph detection
  - A pair of images is analysed - and one is a trusted Bona Fide image
  - Biometric verification (e.g. at the border)



MAD Evaluation

Generalising evaluation - differential scenario

- training on FERET, testing on FRGCv2
  - hand-crafted feature extractors perform well
  - no post-processing of morph images

MAD-method	Classifier	Morphing Algorithm (Training)	Morphing Algorithm (Test)	D-EER
LBP	SVM	Dlib und OpenCV	Dlib und OpenCV	0.0228
LBP (4x4 cells)	SVM	Dlib und OpenCV	Dlib und OpenCV	0.0997
LBP	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0.0645
LBP (4x4 cells)	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0.0471
BSIF	SVM	Dlib und OpenCV	Dlib und OpenCV	0.0775
BSIF (4x4 cells)	SVM	Dlib und OpenCV	Dlib und OpenCV	0.0656
BSIF	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0.0695
BSIF (4x4 cells)	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0.0742
OpenFace	SVM	Dlib und OpenCV	Dlib und OpenCV	0.1253
OpenFace	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0.1373
FaceNet	SVM	Dlib und OpenCV	Dlib und OpenCV	0.1943
FaceNet	AdaBoost	Dlib und OpenCV	Dlib und OpenCV	0.1745
LBP	SVM	FaceMorpher	FaceMorpher	0.0025
LBP (4x4 cells)	SVM	FaceMorpher	FaceMorpher	0.0023
LBP	AdaBoost	FaceMorpher	FaceMorpher	0.0453
LBP (4x4 cells)	AdaBoost	FaceMorpher	FaceMorpher	0.0000
BSIF	SVM	FaceMorpher	FaceMorpher	0.0253
BSIF (4x4 cells)	SVM	FaceMorpher	FaceMorpher	0.0085
BSIF	AdaBoost	FaceMorpher	FaceMorpher	0.0126
BSIF (4x4 cells)	AdaBoost	FaceMorpher	FaceMorpher	0.0695
OpenFace	SVM	FaceMorpher	FaceMorpher	0.1432
OpenFace	AdaBoost	FaceMorpher	FaceMorpher	0.1404
FaceNet	SVM	FaceMorpher	FaceMorpher	0.2054
FaceNet	AdaBoost	FaceMorpher	FaceMorpher	0.1745

MAD Evaluation

Generalising evaluation - differential scenario

- training on FERET, testing on FRGCv2
- now we focus on LBP only
  - and again no post-processing of morph images

MAD-method	Classifier	Morphing Algorithm (Training)	Morphing Algorithm (Test)	D-EER
LBP	SVM	Dlib und OpenCV	FaceMorpher	0.0153
LBP	AdaBoost	Dlib und OpenCV	FaceMorpher	0.0471
LBP	SVM	FaceMorpher	Dlib und OpenCV	0.0251
LBP	AdaBoost	FaceMorpher	Dlib und OpenCV	0.1369

We reach in the best case

- approx 1 % EER (between APCER and BPCER)

MAD Evaluation

Generalising evaluation - differential scenario

- training on FERET, testing on FRGCv2
- now we focus on LBP only
- post-processing of morph images with the sharpening operator

MAD-method	Classifier	Morphing Algorithm (Training)	Morphing Algorithm (Test)	D-EER
LBP	SVM	Dlib und OpenCV	FaceMorpher	0.0108
LBP	AdaBoost	Dlib und OpenCV	FaceMorpher	0.0414
LBP	SVM	FaceMorpher	Dlib und OpenCV	0.0417
LBP	AdaBoost	FaceMorpher	Dlib und OpenCV	0.1289

We still reach in the best case

- approx 1 % EER (between APCER and BPCER)

Future - What needs to be done?

MAD Evaluations on Digital Images

First investigations on morphing attack detection

- are on a small dataset
- Addressing only digital application process (applicable for New Zealand, Estonia, Irland)

The upcoming evaluations

- NIST-FRVT-MORPH evaluation
- SOTAMD evaluation

will provide valuable insights

MAD Evaluations on Digital Images

Our submissions to NIST-FRVT-MORPH / SOTAMD:

- LBP-MAD proposed in [RRB16], [SRB18a] and [SRB18b]
- PRNU-MAD proposed in [DSRUB18a] and [DSRUB18b]

[RRB16] R. Raghavendra, K. Raja, C. Busch: "Detecting Morphed Facial Images", in Proceedings of 8th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS-2016), September 6-9, Niagra Falls, USA, (2016)

[SRB18a] U. Scherhag, C. Rathgeb, C. Busch: "Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), April 24-27, (2018)

[SRB18b] U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)

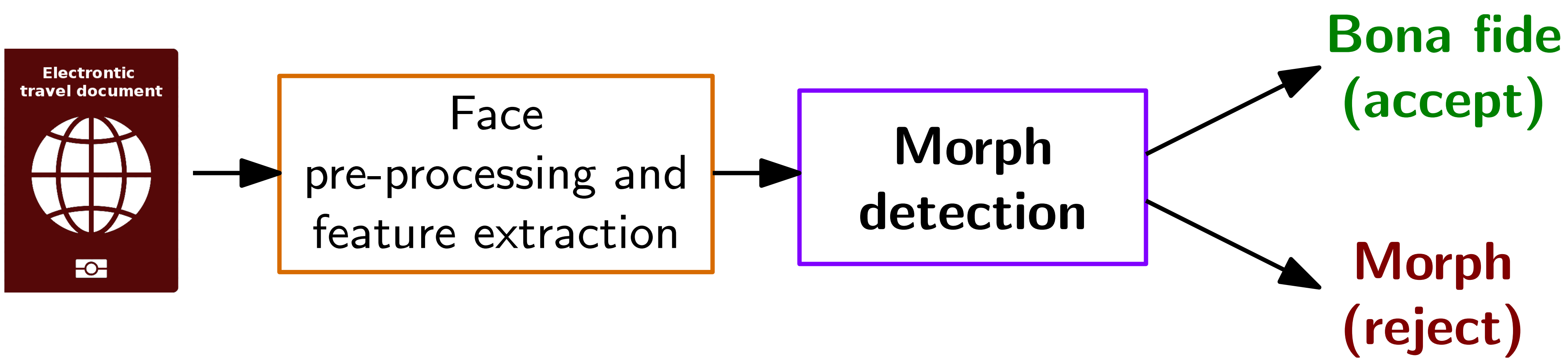
[DSRUB18a] L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, C. Busch: "PRNU-based Detection of Morphed Face Images“, in Proceedings of 6th International Workshop on Biometrics and Forensics (IWBF 2018), Sassari, IT, June 7-8, (2018)

[DSRUB18b] L. Debiasi, C. Rathgeb, U. Scherhag, A. Uhl, C. Busch: "PRNU Variance Analysis for Morphed Face Image Detection“, in Proceedings of 9th International Conference on Biometrics: Theory, Applications and Systems (BTAS 2018), Los Angeles, US, October 22-25, (2018)

MAD Evaluations on Single Digital Images

Our submission to NIST-FRVT-MORPH:

- Classifiers for single image analysis
- No-reference morph detection
  - One single facial image is analysed (e.g. in the passport application office)



MAD Evaluations on Single Digital Images

Our submission to NIST-FRVT-MORPH:

- LBP-MAD classifier for single image analysis
  - no-reference scenario
- feature vector
  - 4 x 4 histograms, 256 values each
  - Normalized histograms
- trained SVM on
  - 1000 original images from FERET and FRGCv2
  - 1000 morphs from FERET and FRGCv2
    - 2 morphing algorithms
    - 4 different post processing methods
- tested on
  - 1000 original images from FERET and FRGC
  - 1000 morphs from FERET and FRGC

We reach BPCER = 5.25% @ APCER = 5.80%

MAD Evaluations on Single Digital Images

Our submission to NIST-FRVT-MORPH:

- PRNU-MAD classifier for single image analysis
  - no-reference scenario
- feature vector
  - Noise residuals
- trained SVM on
  - 1000 original images from FERET and FRGCv2
  - 1000 morphs from FERET and FRGCv2
    - 2 morphing algorithms
    - 4 different post processing methods
- tested on
  - 1000 original images from FERET and FRGC
  - 1000 morphs from FERET and FRGC

We reach BPCER = 5.6% @ APCER = 4.6%

What needs to be Done ?

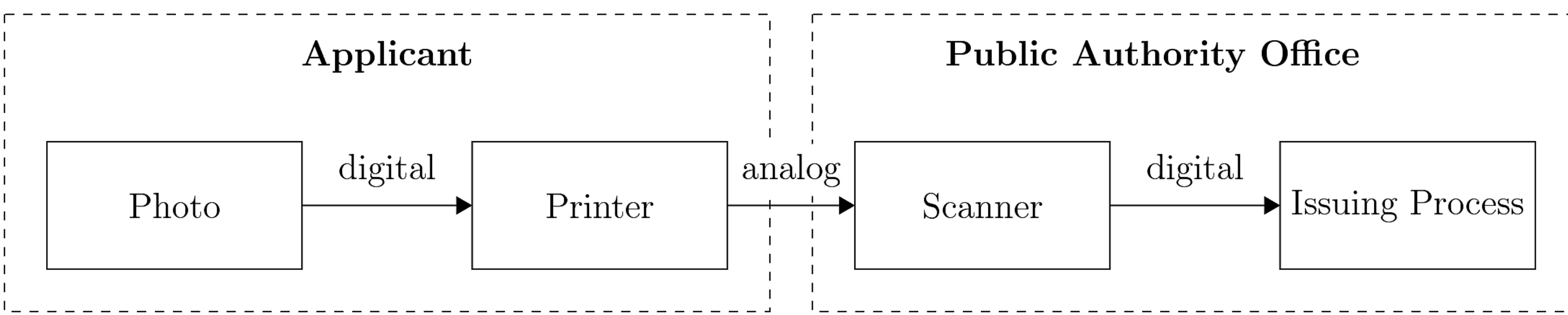
Evaluations must consider the printing process

- There are numerous parameters to explore for this

*result = f (dataset-training, dataset-testing, morphing-attack, landmark-detector, feature-extractor, classifier, scenario (no-reference vs. differential), post-processing, **printer, scanner**)*

Printer / Scanner of choice

Resolution (spatial sampling rate)



What needs to be Done ?

Multiple dimensions to explore:

- Large scale datasets evaluation in NIST FRVT MORPH
- Generalisation on public datasets
  - FERET, FRGCv2, FEI, ARface
- Morphing mechanism
  - Fantamorph, OpenCV, Splicing, GIMP, …
- Number of contributing subjects (broker model)
- The most effective alpha-factor (50:50 or 20:80)
- Random or lookalike morphs
  - Same gender, same skin-color as selection criteria
- Digital samples versus digital-analog-digital transition

References

Publications available https://www.christoph-busch.de/projects-mad.html

- L. Debiasi, C. Rathgeb, U. Scherhag, A. Uhl, C. Busch: "PRNU Variance Analysis for Morphed Face Image Detection“, in Proceedings of 9th International Conference on Biometrics: Theory, Applications and Systems (BTAS 2018), Los Angeles, US, October 22-25, (2018)
- R.Raghavendra, S. Venkatesh, K. Raja, C. Busch: "Detecting Face Morphing Attacks with Collaborative Representation of Steerable Scale-Space Features“, in Proceedings of 3rd International Conference on Computer Vision and Image Processing (CVIP 2018), Japalpur, IN, September 29 - October 1, (2018)
- U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch: "Detecting Morphed Face Images Using Facial Landmarks“, in Proceedings of International Conference on Image and Signal Processing (ICISP 2018), Cherbourg, FR, July 2-4, (2018)
- U. Scherhag, C. Rathgeb, C. Busch: "Performance Variation of Morphed Face Image Detection Algorithms across different Datasets“, in Proceedings of 6th International Workshop on Biometrics and Forensics (IWBF 2018), Sassari, IT, June 7-8, (2018)
- L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, C. Busch: "PRNU-based Detection of Morphed Face Images“, in Proceedings of 6th International Workshop on Biometrics and Forensics (IWBF 2018), Sassari, IT, June 7-8, (2018)
- U. Scherhag, C. Rathgeb, C. Busch: „Detection of Morphed Faces from Single Images: a Multi-Algorithm Fusion Approach“, in Proceedings if of the 2nd International Conference on Biometric Engineering and Applications (ICBEA 2018), Amsterdam, The Netherlands, May 16-18, (2018)
- U. Scherhag, C. Rathgeb and C. Busch: „Towards Detection of Morphed Face Images in electronic Travel Documents“, in Proceedings of the 13th IAPR International Workshop on Document Analysis Systems (DAS 2018), Vienna, Austria, April 24-27, (2018)
- M. Gomez-Barrero, C. Rathgeb, U. Scherhag, C. Busch: „Predicting the Vulnerability of Biometric Systems to Attacks based on Morphed Biometric Samples“, in IET Biometrics, (2018)
- C. Rathgeb, C. Busch: "On the Feasibility of Creating Morphed Iris-Codes", in Proceedings of International Joint Conference on Biometrics (IJCB 2017), Denver, Colorado, October 1-4, (2017)
- R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Face Morphing Versus Face Averaging: Vulnerability and Detection", in Proceedings of International Joint Conference on Biometrics (IJCB 2017), Denver, Colorado, October 1-4, (2017)
- U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 20-22, (2017)
- R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)
- M. Gomez-Barrero, C. Rathgeb, U. Scherhag, C. Busch: "Is Your Biometric System Robust to Morphing Attacks?", in Proceedings of 5th International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, April 4-5, (2017)
- U. Scherhag, R. Raghavendra, K. Raja, M. Gomez-Barrero, C. Rathgeb, C. Busch: "On The Vulnerability Of Face Recognition Systems Towards Morphed Face Attacks", in Proceedings of 5th International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, April 4-5, (2017)
- R. Raghavendra, K. Raja, C. Busch: "Detecting Morphed Facial Images", in Proceedings of 8th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS-2016), September 6-9, Niagra Falls, USA, (2016)
- M. Ferrara, A. Franco, D. Maltoni: “On the Effects of Image Alterations on Face Recognition Accuracy”, in Face Recognition Across the Imaging Spectrum, Springer Nature, (2016)
- M. Ferrara, A. Franco, D. Maltoni: “The magic passport”, in Proceedings IEEE International Joint Conference on Biometrics, (2014)

Sponsors

This research is kindly sponsored by

- Federal Office for Information Security (BSI)
  - FACETRUST

Federal Office
for Information Security

- Center for Research in Security and Privacy:
  - LOEWE/BMBF CRISP http://www.crisp-da.de/

CRISP
Center for Research
in Security and Privacy

- Norwegian Research Council
  - IKTPLUSS SWAN http://nislab.no/biometrics_lab/swan

Forskningsrådet

- Norwegian University of Science and Technology

NTNU

Contact

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: `christoph.busch@ntnu.no`
Phone: +47-611-35-194

Contact

CRISP
Center for Research
in Security and Privacy

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@crisp-da.de

Telefon +49-6151-16-30090
www.dasec.h-da.de
www.crisp-da.de